



Homeland
Security

Daily Open Source Infrastructure Report

26 March 2015

Top Stories

- A Romanian national was extradited to the U.S. March 20 to face charges that he allegedly led a large-scale hacking scam in which he breached computer systems of retailers, medical offices, security companies, and individuals' online accounts. – *NJ.com* (See item [4](#))
- Officials are investigating the source of a leak that is causing the loss of more than 600,000 gallons of water a day in Rutland, Vermont, and has been affecting customers' water pressure since March 21. – *Associated Press; Rutland Herald* (See item [17](#))
- Swedesboro-Woolwich School District in New Jersey is investigating an attack on its computer network after discovering March 21 that the network was down when they received a ransom message. – *South Jersey Times* (See item [18](#))
- The mayor of the District of Columbia announced March 24 that repair work began on Washington, D.C.'s emergency computer system used to dispatch firetrucks and ambulances, and that additional ambulances and other precautions will be put in place in order to help mitigate the troubled system. – *Washington Post* (See item [20](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *March 24, Dickinson Press* – (North Dakota) **Halliburton to close Minot facility.** Officials at Halliburton reported March 24 that operations will be suspended at its Minot site and that the facility will be closed effective April 1 due to changing business needs from consumers.
Source: <http://www.thedickinsonpress.com/news/north-dakota/3707037-halliburton-close-minot-facility>

For another story, see item [25](#)

[\[Return to top\]](#)

Chemical Industry Sector

Nothing to report

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

2. *March 24, Kennewick Tri-City Herald* – (National) **DOE to look at separate disposal of defense, commercial nuclear waste.** The U.S. President authorized the U.S. Department of Energy (DOE) to begin developing a national repository for high-level radioactive defense waste March 24, and the DOE announced plans to start with one or more temporary storage facilities for commercial waste at sites volunteered with State and community consent.
Source: http://www.tri-cityherald.com/2015/03/24/3477644_doe-to-look-at-separate-disposal.html

[\[Return to top\]](#)

Critical Manufacturing Sector

3. *March 25, Reuters* – (International) **Ford recalls over 220,000 vehicles in North America for three issues.** Ford Motor Co., announced March 25 a recall for 194,484 model years 2011 – 2013 Ford Explorer SUVs and Police Interceptor utility vehicles in the U.S. for a spring issue that could cause doors to unlatch in a side-impact crash, and a recall for 1,586 model years 2013 – 2015 Lincoln MKT limo and hearse vehicles for a vacuum pump relay issue that could cause an underhood fire. The company also included 6,472 model years 2011 – 2013 F-Series Super Duty ambulance vehicles and a 6.7-liter diesel engine version from model years 2014 – 2015 in the recall due to an exhaust gas temperature sensor issue that could fail to detect a high temperature condition.
Source: <http://www.msn.com/en-us/news/us/ford-recalls-over-220000-vehicles-in-north-america-for-three-issues/ar-AA9YYKI>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

4. *March 23, NJ.com* – (International) **Alleged hacker brought to N.J. on charges of large-scale identity theft.** A Romanian national was extradited to the U.S. March 20 to face charges that he allegedly oversaw a large-scale computer hacking scheme in which he breached computer systems of retailers, medical offices, security companies, and individuals' online accounts to obtain several thousand user names, passwords, and payment card numbers from 2011 – 2014, including 10,000 credit and debit cards from one victim alone.

Source:

http://www.nj.com/news/index.ssf/2015/03/alleged_hacker_brought_to_nj_on_charges_of_large-s.html

For another story, see item [18](#)

[\[Return to top\]](#)

Transportation Systems Sector

5. *March 25, WKMG 6 Orlando* – (Florida) **Interstate 4 reopens in Volusia County.** Eastbound lanes of Interstate 4 near DeLand were closed for several hours March 25 due to 2 separate crashes involving 7 vehicles that blocked the roadway near mile marker 125. The accidents remain under investigation.
Source: <http://www.clickorlando.com/news/crash-closes-i4-in-volusia-county/32000984>
6. *March 25, Associated Press* – (Massachusetts) **Tanker truck crash shuts down Bourne Rotary, bridge.** The Massachusetts Department of Environmental Protection reported that a semi-truck carrying fuel overturned and spilled about 5,000 gallons of gasoline onto a grassy infield of the Bourne Rotary and into catch basins that connect to the Cape Cod Canal prompting the closure of the rotary and the Bourne Bridge for more than 10 hours while crews cleaned the scene March 24.
Source: http://www.bostonherald.com/news_opinion/local_coverage/2015/03/tanker_truck_crash_shuts_down_bourne_rotary_bridge
7. *March 24, Waxahachie Daily Light* – (Texas) **Semi-truck fire shuts down southbound I-35E for 4 hours.** A semi-truck fire that sparked a small grassfire shut down both southbound lanes of Interstate 35E in Milford for 4 hours March 24 while

firefighters extinguished the blaze and HAZMAT crews cleared the scene. Authorities are investigating what caused the fire and where it originated within the semi-truck.

Source: http://www.waxahachietx.com/news/ellis_county/semi-truck-fire-grassfire-shut-down-interstate-at-milford/article_5cf2e211-3f4e-5026-a33e-4786498d26f5.html

8. *March 25, KDVR 31 Denver* – (Colorado) **One driver critically injured after 3-vehicle crash involving two semis shuts down I-70.** Westbound Interstate 70 was closed for more than 2 hours at Airport Boulevard in Aurora, Colorado, March 24 following a 3-vehicle accident involving 2 semi-trucks. Three individuals were transported to area hospitals for injuries sustained during the crash.
Source: <http://kdvr.com/2015/03/24/westbound-i-70-shut-down-at-tower-road-after-truck-crash/>
9. *March 24, WITI 6 Milwaukee* – (Wisconsin) **Three people injured in early morning crash on Highway 14 in Walworth County.** Highway 14 in the Town of Walworth was closed in both directions for almost 4 hours due to a crash involving a semi-truck and 2-vehicles that injured 3 people March 24. The crash remains under investigation.
Source: <http://fox6now.com/2015/03/24/three-people-injured-in-early-morning-crash-on-highway-14-in-walworth-county/>
10. *March 24, KING 5 Seattle* – (Washington) **Highway 99 southbound open after overturned semi closed it for hours.** All southbound lanes of State Route 99 near the Alaskan Way Viaduct in Seattle were shut down for 9 hours after a semi-truck carrying fish overturned causing the contents of the trailer to shift and rendering it unstable to transport. Passengers disembarked buses that were stuck in traffic to walk off the viaduct, and authorities reversed traffic flow so drivers could exit the viaduct via on-ramps.
Source: <http://www.king5.com/story/news/local/seattle/2015/03/24/overturned-semi-shuts-down-southbound-highway-99/70396698/>

[\[Return to top\]](#)

Food and Agriculture Sector

11. *March 25, WDAZ 8 Devil's Lake* – (North Dakota) **Man arrested in fatal Bottineau County shooting.** Bottineau County officials arrested a suspect in the March 24 shooting at the Turtle Mountain Pork hog farm near Landa that left two people dead. Area schools went into lockdown while authorities investigated the incident.
Source: <http://www.wdaz.com/news/3706750-update-man-arrested-fatal-bottineau-county-shooting>
12. *March 24, U.S. Food and Drug Administration* – (National) **Superior Foods, Inc., of Watsonville, CA is recalling 8,475 cases of Simply Balanced 10-oz frozen Organic Chopped Spinach distributed exclusively at Target stores.** The U.S. Food and Drug Administration reported March 24 that Superior Foods, Inc., recalled 8,475 cases of its Simply Balanced Organic Chopped Spinach that was distributed exclusively at Target stores nationwide after the company received a notice from its supplier that it may have

received organic spinach with the possible presence of *Listeria monocytogenes*.

Source: <http://www.fda.gov/Safety/Recalls/ucm439761.htm>

13. *March 24, U.S. Food and Drug Administration* – (National) **Twin City Foods, Inc. recalls frozen Cadia Organic Cut Spinach, Meijer Organics Chopped Spinach, Wild Harvest Organic Cut Leaf Spinach, and Wegmans Organic Just Picked Spinach because of possible health risk.** The U.S. Food and Drug Administration announced March 24 that Twin City Foods, Inc., recalled Cadia Organic Cut Spinach, Meijer Organics Chopped Spinach, Wild Harvest Organic Cut Leaf Spinach, and Wegmans Organic Just Picked Spinach after Coastal Green Vegetable Company LLC, a supplier for the products, initiated a recall for bulk spinach due to possible *Listeria monocytogenes* contamination. The recalled products were distributed to warehouses in several States.
Source: <http://www.fda.gov/Safety/Recalls/ucm439755.htm>
14. *March 24, U.S. Food and Drug Administration* – (National) **Carmel Food Group recalls 3 frozen ravioli items under Rising Moon Organics label – due to possible health risk.** The U.S. Food and Drug Administration reported March 24 that Carmel Food Group issued a voluntary recall for certain Rising Moon Organics frozen ravioli products after a supplier notified the company that spinach used during the manufacturing process may have been contaminated with *Listeria monocytogenes*. The products were distributed through retailers nationwide.
Source: <http://www.fda.gov/Safety/Recalls/ucm439539.htm>
15. *March 24, U.S. Food and Drug Administration* – (National) **Giant Eagle voluntarily recalls Japanese Breaded Cod Fillets due to an undeclared soy allergen.** The U.S. Food and Drug Administration announced March 23 a recall for all lots of Giant Eagle brand Japanese Breaded Cod Fillets due to undeclared soy. The recalled products were prepared and sold individually from the Seafood department inside Giant Eagle and Market District supermarkets in several States
Source: <http://www.fda.gov/Safety/Recalls/ucm439658.htm>
16. *March 24, U.S. Food and Drug Administration* – (Pennsylvania; Ohio) **Giant Eagle voluntarily recalls Little Italy Paninis due to an undeclared egg allergen.** The U.S. Food and Drug Administration announced March 23 a recall for all lots of Giant Eagle brand Little Italy Paninis prepared and sold individually from the Prepared Foods department inside Giant Eagle and Market District supermarkets in Pennsylvania and Ohio due to undeclared egg.
Source: <http://www.fda.gov/Safety/Recalls/ucm439643.htm>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

17. *March 25, Associated Press; Rutland Herald* – (Vermont) **Vermont city losing 600K-plus gallons of water daily in leak.** Officials are investigating the source of a leak that is causing the loss of more than 600,000 gallons of water a day in Rutland, Vermont,

and has been affecting customers' water pressure since March 21. The city's Public Works Commissioner reported that workers are inspecting valves, hydrants, and vacant buildings, and announced a plan to isolate and check 3 transmission lines running from a water plant into the city.

Source: <http://abcnews.go.com/US/wireStory/vermont-city-losing-600k-gallons-water-daily-leak-29892445>

[\[Return to top\]](#)

Healthcare and Public Health Sector

See item [4](#)

[\[Return to top\]](#)

Government Facilities Sector

18. *March 24, South Jersey Times* – (New Jersey) **School district 'bitcoin hostage' situation continues; FBI, Homeland Security investigating.** Swedesboro-Woolwich School District in New Jersey is investigating an attack on its computer network which caused them to postpone exams after discovering March 21 that their entire network was down when they received a ransom message requesting 500 bitcoins. The district restored encrypted files and is in the process of restoring its servers to remove the malware after email communications, online resources for an exam, Excel spreadsheets, and Adobe PDF files were breached as well.

Source: http://www.nj.com/gloucester-county/index.ssf/2015/03/school_district_bitcoin_hostage_situation_continue.html

[\[Return to top\]](#)

Emergency Services Sector

19. *March 25, WFAA 8 Dallas* – (Texas) **Ambulance stolen from Kaufman hospital.** An emergency room patient from Texas Health Presbyterian Hospital in Kaufman stole an ambulance March 24 and led police on a short pursuit that ended near Kemp when officers laid spike strips on the road and deflated the ambulance's tires. The suspect was taken into custody without further incident.

Source: <http://www.wfaa.com/story/news/crime/2015/03/24/ambulance-stolen-from-presbyterian-hospital-kaufman/70389330/>

20. *March 24, Washington Post* – (Washington, D.C.) **Widespread problems hampering new 911 fire dispatch system in D.C.** The mayor of the District of Columbia announced March 24 that repair work began on Washington, D.C.'s emergency computer system used to dispatch firetrucks and ambulances, and that additional ambulances and other precautions will be put in place in order to help mitigate the troubled system. Authorities found that the system has repeatedly malfunctioned since it was installed in the fall of 2014, slowing response time for emergency personnel.

Source: http://www.washingtonpost.com/local/dc-politics/widespread-problems-hampering-new-911-fire-dispatch-system-in-dc/2015/03/24/345e16d0-d23c-11e4-a62f-ee745911a4ff_story.html

21. *March 24, San Francisco Bay City News* – (California) **Internal investigation launched into how jail inmate escaped.** The San Francisco Police Department is searching for an inmate facing charges who escaped from the county jail at the Hall of Justice March 23 while he was being escorted to take out the trash. Authorities stated that an internal investigation was underway to determine changes in protocol for officers.

Source: <http://www.sfexaminer.com/sanfrancisco/sf-sheriffs-deputies-police-search-for-escaped-inmate/Content?oid=2924496>

[\[Return to top\]](#)

Information Technology Sector

22. *March 25, Securityweek* – (International) **Over 15,000 vulnerabilities detected in 2014: Secunia.** Secunia released its annual vulnerability review and found that 15,435 vulnerabilities across 3,870 applications from 500 vendors were discovered in 2014, 11 percent of which were considered highly critical while .3 percent were rated extremely critical. The report also states that over 60 percent of attacks occurred through remote networks making it the most common attack vector, among other trends.

Source: <http://www.securityweek.com/over-15000-vulnerabilities-detected-2014-secunia>

23. *March 25, Help Net Security* – (International) **Half of all Android devices vulnerable to installer hijacking attacks.** Security researchers at Palo Alto Networks discovered that a critical Android vulnerability discovered over a year ago and dubbed “Android Installer Hijacking”, can allow attackers to completely compromise devices by changing or replacing seemingly legitimate applications with malware during installation without users’ knowledge. The flaw affects all devices running Android versions 4.2 and earlier, and some running version 4.3.

Source: <http://www.net-security.org/secworld.php?id=18133>

24. *March 24, Softpedia* – (International) **Yebot backdoor built for wide range of malicious operations.** Security researchers from Dr.Web discovered that a backdoor trojan dubbed Yebot can run file transfer protocol (FTP) and socket secure (SOCKS) 5 proxy servers, gain remote access to systems through a remote desktop protocol (RDP), capture keystrokes and screenshots, intercept system functions, change code of running processes, search for private keys, and intercept all features associated with Web browsing. The trojan infects computers by injecting code into four Microsoft Windows processes before downloading and decrypting its contents and running in memory.

Source: <http://news.softpedia.com/news/Yebot-Backdoor-Built-for-a-Slew-of-Malicious-Operations-476654.shtml>

25. *March 24, Softpedia* – (International) **Leaked full version of NanoCore RAT used to target energy companies.** Security researchers at Symantec identified that approximately 40 percent of systems infected by the widely-available NanoCore remote access trojan (RAT) delivered by a malicious rich text format (RTF) or Microsoft Word file that exploits an old vulnerability in Windows Common Controls ActiveX component since January 2014 were in the U.S., while cyber-criminals have been employing the malware in targeted attacks on energy companies in Asia and the Middle East since March 6.

Source: <http://news.softpedia.com/news/Leaked-Full-Version-of-NanoCore-RAT-Used-to-Target-Energy-Companies-476606.shtml>

26. *March 24, Softpedia* – (International) **Over 22.5 million PUAs detected last month by antivirus vendor.** Germany-based Avira reported that the company's antivirus software detected over 22.5 million potentially unwanted applications (PUAs) and highlighted five as the most prevalent in February that could inject malicious code, request sensitive information from users, or extract information without their consent.

Source: <http://news.softpedia.com/news/Over-22-5-Million-PUAs-Detected-Last-Month-by-Antivirus-Vendor-476650.shtml>

For another story, see item [4](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

See item [23](#)

[\[Return to top\]](#)

Commercial Facilities Sector

27. *March 25, Tucson News Now* – (Arizona) **Firefighter injured, 30 displaced in southeast-side apartment fire.** Thirty residents were displaced following a March 25 fire at a Tucson apartment building that resulted in a structure collapse. Residents from adjoining apartment buildings were evacuated as a precaution, and three individuals were transported to area hospitals with minor injuries.

Source: <http://www.tucsonnewsnow.com/story/28609890/firefighter-injured-30-displaced-in-east-side-apartment-fire>

28. *March 24, Pittsburgh Post-Gazette* – (Pennsylvania) **Wilmerding residents may be**

displaced at least a week. Nineteen residents of the Wilmerding Apartments building in Pennsylvania were displaced March 22 following a waterline break that caused water to enter the building's electrical system and prompted officials to shut off power and evacuate residents. Officials reported that it could take at least 1 week to make plumbing and electrical repairs before inspections can be completed and residents can return to the building.

Source: <http://www.post-gazette.com/local/east/2015/03/24/Water-leak-damage-may-displace-Wilmerding-apartment-residents-at-least-a-week/stories/201503240092>

29. *March 23, KCBA 35 Salinas* – (California) **Food Bank for Monterey Co suffers huge fire loss.** The Food Bank for Monterey County suffered an estimated \$500,000 in damage to its fleet of refrigerated food distribution trucks following a March 21 fire that appeared to have been intentionally set. Food deliveries were halted indefinitely until alternative transportation is acquired.

Source: <http://www.kcba.com/2015/03/23/76545/>

For another story, see item [4](#)

[\[Return to top\]](#)

Dams Sector

30. *March 24, Associated Press* – (West Virginia) **Clarksburg water board OKs removal of 3 state dams.** The Clarksburg Water Board voted March 23 to enter an agreement with the U.S. Fish & Wildlife Service to allow the agency to begin the permitting process for the removal of 3 dams along the West Fork River. The process is estimated to take about 90 days and the removal is planned to begin in the summer.

Source: <http://www.wvgazette.com/article/20150324/GZ01/150329620>

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.